



Remote Feature Activation

Getting Started with Remote Feature
Activation (RFA)

03-300484
Issue 2.4
June 2006

Contents

About this book	7
What's new in this version of Getting Started With RFA?	7
Audience	7
Downloading this book and updates from the Web	8
Downloading this book	8
Conventions	8
General	8
Typography	8
Commands	9
User input	9
System output and field names	9
Trademarks	9
Trademarks and Service Marks	10
Technical assistance	11
Within the United States	11
International	11
Sending us comments	12
Chapter 1: Remote Feature Activation Overview	13
User requirements	13
Design configuration	14
Reliability and availability	14
Registration	14
Registration for Avaya Associates	14
Registration for Avaya BusinessPartners	15
Group Authorization Identification (GAI)	16
Training	16
Feature Keywords	16
Value types	17
Host IDs and serial numbers	17
RFA Swap-Out functionality	17
Pre-installation and application readiness checklist	18
RFA help	19
Chapter 2: Important Product Information	21
Advanced IP Phone Features	21
Advanced IP Phone Features license file information	22

Contents

Application Assurance Networking	23
Application Assurance Networking license file information	23
Application Design Environment	25
RFA licensed ADE components	25
ADE license file information	26
Application Enablement (AE) Services.	27
Upgrading to AE	28
Upgrading CVLAN R9 to AE.	28
Upgrading DEFINITY LAN Gateway to AE	28
CVLAN Server 9.0 for Linux.	29
RFA licensed AE applications	29
AE license file information	30
Branch Gateways	32
The serial number for the G250 or G350 Media Gateway	33
Post installation verification	33
Activating the VPN.	33
Branch Gateway license file information.	34
Communication Manager	34
Serial numbers for Communication Manager	35
Working with authentication files.	35
DEFINITY upgrades	36
DEFINITY migrations	36
The Shared Blade Server	37
Interaction Center	38
E-mail license request and IC.	39
IC license file information	40
Integrated Management	43
Integrated Management license file information	43
Meeting Exchange	44
Meeting Exchange license file information	45
Modular Messaging	45
Host ID information	46
Post installation verification	46
Modular Messaging license information	46
Personal WorkSpace	47
PWS licensing information	48
Security Gateway	48
Security Gateway models	49
Security Gateway license file information	50

SIP Enablement Services	50
SIP Enablement Services module type.	51
Post installation verification	51
SIP Enablement Services license file information.	51
Softclients	52
Softclients Host ID information	52
Softclients license file information	52
Unified Communication Center	53
UCC Host ID information	54
UCC license file information	55
Voice Self Service (VSS).	55
VSS Host ID information	56
VSS license file information.	56
Glossary	59
Index	61

About this book

Note:

Every attempt is made to ensure the accuracy of the contents of this document. However, many components are subject to change because of the evolving needs of the business.

The Getting Started With Remote Feature Activation (RFA) guide has been developed to provide information about RFA supported products in RFA. It is not intended to replace high-level technical information that is available from various documentation guides.

This document is to be used by Avaya Services and Avaya BusinessPartners as an aid to:

- Understand the terms and procedures used in RFA
- Clarify the responsibilities of the RFA user
- Identify the browser requirements for accessing RFA
- Provide basic general directions for accessing and using RFA
- Provide information for each Avaya family supported by RFA

Please read this Getting Started With RFA guide before attempting to implement a solution for an RFA supported product.

What's new in this version of Getting Started With RFA?

Version 2.3 of the Getting Started With Remote Feature Activation (RFA) contains information on a new product family, Meeting Exchange.

Audience

This book is for the sales person, technicians, or other personnel requiring knowledge on RFA supported products.

Downloading this book and updates from the Web

You can download the latest version of this book from the Avaya Web site. You must have access to the Internet and a copy of Acrobat Reader.

Avaya makes every effort to ensure that the information in this book is complete and accurate. However, information can change after we publish this book. Therefore, the Avaya Web site might also contain new product information and updates to the information in this book. You also can download these updates from the Avaya Web site.

Downloading this book

To download the latest version of this book:

1. Access the Avaya Support web site at <http://support.avaya.com>.
2. Click Find Documentation and Download by Product Name.
3. Click on the R in the alphabet list.
4. Select the document from the list.

Note:

This book is only available in PDF format.

Conventions

This section describes the conventions used in this book.

General

The commands and screens are from the newest Avaya systems. The books referenced are the most current books at the time of this writing. You can substitute the appropriate commands for your system and see the books that you have available.

Typography

This section describes the typographical conventions for commands, keys, user input, system output, and field names.

Commands

- Commands are in **bold** type.
Example
Type **statuslicense** and press **Enter**.
- Command options are in **bold** type inside square brackets.
Example
At the DOS prompt, type **copybcf [-F34]**.

User input

- User input is in **bold** type, whether you must type the input, select the input from a menu, or click a button or similar element on a screen or a Web page.
Examples
 - Type **exit**, and then press **Enter**.
 - On the **File** menu, click **Save**.
 - On the Network Gateway page, click **Configure > Hardware**.

System output and field names

- System output and field names on the screen are in `monospaced` type.
Examples
 - The system displays the following message:
`The installation is in progress.`
 - Type **y** in the **Message Transfer?** field.

Trademarks

All trademarks identified by the ® or ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.

Trademarks and Service Marks

The following are trademarks or registered trademarks of Avaya:

- AUDIX®
- Cajun®
- Callvisor®
- Callmaster®
- CentreVu™
- CONVERSANT®
- DEFINITY®
- DIMENSION®
- INTUITY™
- MERLIN®
- MultiVantage™
- Softconsole™
- TransTalk®
- VOICE POWER®

The following are trademarks or registered trademarks of Lucent Technologies:

- 5ESS™, 4ESS™

The following are trademarks or registered trademarks of AT&T:

- ACCUNET®
- DATAPHONE®
- MEGACOM®
- MULTIQUEST®
- TELESEER®

The following are trademarks or registered trademarks of other companies:

- Acrobat® (registered trademark of Adobe Systems Incorporated)
- Ascend® (registered trademark of Ascend, Inc.)
- Audichron® (registered trademark of Audichron Company)
- MS-DOS® (registered trademark of the Microsoft Corporation)
- MicroChannel® (registered trademark of IBM Systems)

- Microsoft® (registered trademark of Microsoft Corporation)
- MULTIQUEST® (registered trademark of Telecommunications Service)
- NetMeeting® (registered trademark of Microsoft Corporation)
- PagePac® (trademark of the Dracon Division of the Harris Corporation)
- PictureTel® (registered trademark of PictureTel Corporation)
- ProShare® (registered trademark of Intel Corporation)
- UNIX® (trademark of the Novell Corporation)
- Zydacron (registration pending for Zydacron Corporation)

Technical assistance

Avaya provides the following resources for technical assistance.

Within the United States

For help with:

- Feature administration and system applications, call the Avaya Technical Consulting System Support (TCSS) at, 1-800-225-7585
- Maintenance and repair, call the Avaya National Customer Care Support Line at 1-800-242-2121
- Toll fraud, call Avaya Toll Fraud Intervention at 1-800-643-2353

International

For all international resources, contact your local Avaya authorized dealer for additional help.

Sending us comments

Avaya welcomes your comments about this book. To reach us by:

- Mail, send your comments to:

Avaya Inc.
Product Documentation Group
Room B3-H13
1300 W. 120th Ave.
Westminster, CO 80234 USA

- E-mail, send your comments to:

document@avaya.com

- Fax, send your comments to:

1-303-538-1741

Be sure that you mention the name of this book, *Avaya Getting Started With Remote Feature Activation (RFA)*.

Chapter 1: Remote Feature Activation Overview

Remote Feature Activation (RFA) is a web-based application that is used to create and deliver license files for Avaya products. The license files are created using information from the customer and the SAP order. The SAP ordering information can be entered directly into SAP or Avaya and Avaya BusinessPartners can use the Order Messaging/OA Price Tool.

User requirements

To meet the requirements to access RFA you must:

- Be one of the following:
 - An Avaya associate or designee with a valid Avaya HRID number. This requirement also includes the Variable Workforce associates.
 - An approved BusinessPartner with a valid BusinessPartner number.
 - An approved Avaya contractor. This individual typically works for Avaya without a valid HRID number.
- Have a computer equipped with:
 - Internet Explorer 5.0 or later
 - 128 bit encryption
 - Internet access to the RFA web site
 - The supported monitor resolution of 800 X 600
- Be registered and authenticated for each of the Avaya products in which you wish to create or modify a license file:
 - To be registered means you have been given a SSO (Single Sign On) login and are identified in the RFA database.
 - To be authenticated means that your coach or your Avaya Group Authorization Identification (GAI) manager has approved your access to RFA. For information on what a GAI is see [Group Authorization Identification \(GAI\)](#) on page 16.

Design configuration

RFA does not provide design configurations. Avaya configurations must continue to be engineered using the existing tools and processes. The RFA process begins with an approved and accurate SAP order. A correct SAP order is key to the successful creation of the license file.

Reliability and availability

RFA has been designed for high reliability and high availability. RFA is normally available 24 hours a day, seven days a week. However, please be aware that there are factors that exist that will limit RFA availability for up to twelve hours at a time. These factors include maintenance, interactions with other systems that are not available, etc. The times for scheduled RFA outages are posted on the RFA Information page at <http://rfa.avaya.com>. Please check the RFA Information page regularly for the most current information.

Note:

It is highly recommended that you create a license file as soon as you have all the needed information. Do not wait until the day of installation to obtain the license file.

Registration

This section explains how to register for RFA for Avaya Associates and BusinessPartners.

Registration for Avaya Associates

To log on to RFA you must have a valid Single Sign On (SSO) login and password. The SSO system provides access security for many Avaya applications, including RFA. You do not have to register for a SSO login if you are an Avaya associate.



Important:

Check your personal information in RFA for accuracy. Make sure your POST information is correct.

Complete the following steps to register in RFA for a product family:

1. Access the RFA web site at <http://rfa.avaya.com>. This link takes you to the SSO login site.
2. After you enter your SSO login and password the RFA Information page appears.
3. Click **Register to Use RFA for a product family**.
4. Select the product family from the drop-down menu:
 - Select the job function that most closely resembles the job function that you perform. You can find a detailed description for each job function on the RFA Information page under the **RFA Job Function Descriptions** link.
 - Complete the required information and click **Submit**.
 - Your coach automatically receives an e-mail that must be approved before you can become an RFA user.

Registration for Avaya BusinessPartners

To log onto RFA you must have a valid Single Sign On (SSO) login and password. The SSO system provides access security for many Avaya applications, including RFA.

Make sure that your business card information is correct. The business card information is the same as your SSO information. Ensure that your e-mail address is accurate. You can update this information from the SSO login screen.

Complete the following steps to register for a product family:

1. Access the RFA web site at <http://rfa.avaya.com>. This link takes you to the SSO login site. If you already have a SSO login, enter your login and password. If you do not have a SSO login, click **New User** and complete the required information.

After you enter your SSO login and SSO password the system displays the RFA Information page.

2. Click **Register to Use RFA for a product family** and select the product family from the menu:
3. Select one of the following user types:
 - **Tier 1 BusinessPartner** if you purchase directly from Avaya.
 - **Tier 2 BusinessPartner** if you purchase from a Tier 1 BusinessPartner.
 - **Contractor** if you are a contractor working for Avaya and do not have an Avaya HRID number.
4. Enter a Group Authorization Identification (GAI) number. Click **Show GAI Name** to verify that you entered the correct GAI. For more information on GAI, see [Group Authorization Identification \(GAI\)](#) on page 16.
5. Enter the e-mail address that your company provided to Avaya to receive the RFA generated e-mail. RFA uses this e-mail address to e-mail your request to access RFA to your company. Avaya must receive a reply to the e-mail before you can become an authenticated RFA user.

Group Authorization Identification (GAI)

A GAI is a unique number assigned to each BusinessPartner in RFA. This number is included on the system record of each license. A BusinessPartner must have their GAI on a system record in order to access it. The GAI for a Tier II BusinessPartner is available from the Tier I BusinessPartner. During the creation of a system record, the Tier I BusinessPartner must include the Tier II BusinessPartner's GAI. Should a BusinessPartner require access to a system record that does not contain their GAI, they can complete a form called **Transfer System Record to a Different BP** located on the RFA Information page.

Training

The detailed instructions on how to use RFA for each product family can be found in the *Avaya Remote Feature Activation (RFA) User Guide* located at <http://support.avaya.com>. You should read the RFA User Guide shortly before an upcoming installation to ensure you can apply the knowledge that you obtained.

Feature Keywords

RFA creates a license file based on the material codes that appear in the SAP order. RFA maps between the SAP material codes and the features and capacities in the license file. While the license file does not contain the material codes themselves, it does contain the features and the capacities that will be activated for the system. The features and capacities are represented by Feature Keywords. Feature Keywords are English text that uniquely identify which features and capacities to activate. A list of Feature Keywords for each RFA supported product, except Communication Manager, can be found in [Chapter 2: Important Product Information](#) on page 21. For a complete listing of the Communication Manager Keywords see the RFA Information page at <http://rfa.avaya.com>.

Value types

Each feature, feature capacity, or customer entitlement, falls into one of the following types.

- Type I: The Type I Features table contains the software features that are entitlements and the features that are purchased by the customer. Type I features have an on and off, or a yes and no setting.
- Type II: The Type II Features table contains features that have a value or capacity. For some Feature Keywords, the Setting column can be used to set the value for the Feature Keyword.
- Type III: The Type III Features Table contains registration features that have a product ID, a release, and a capacity setting.

Host IDs and serial numbers

RFA uses either the Host ID or the serial number to identify the Avaya product. Each Host ID or serial number must be unique within its product group and therefore can only be used once. You may use the same Host ID or serial number for multiple RFA licenses if the licenses are created for different products.

For more information on which product family uses a Host ID or a serial number, see [Chapter 2: Important Product Information](#) on page 21.

RFA Swap-Out functionality

The RFA Swap-Out functionality is used when a licensed server needs to be replaced. The Swap-Out functionality creates a new RFA system record that contains the new Host ID or the serial number.

All RFA supported products use the Swap-Out functionality. For Communication Manager and Branch Gateways, an authenticated user can perform the swap-out. For all other RFA supported products, the RFA Swap-Out functionality can only be performed by a Tier III Avaya Global Services associate. Use the following information to contact an Avaya support center:

- Avaya technician call 1-800-248-1234
- Avaya BusinessPartner call 877-295-0099
- For international please refer to the following URL to locate your international support center: http://support.avaya.com/japple/css/japple?PAGE=OpenPage&temp.template.name=Support_Countries

Pre-installation and application readiness checklist

[Table 1](#) contains information that you need to obtain before accessing RFA to create or update a license file.

Table 1: Readiness checklist

Item	Completed
SAP order number	
Host ID or serial number	
RFA Transaction number or activity	
Email address of person receiving license file (if applicable)	
SID (if this is an addition or an upgrade)	
Complete Tier I, Tier II, and end-user customer information	

RFA help

There may be times when you need help with RFA or with a RFA license file. The organization that you call for help depends on the type of problem you are experiencing. [Table 2](#) shows examples of the types of problems for which each Helpdesk provides support.

Table 2: Who to call for support

Organization	What they support
The IT Helpdesk	• The RFA application, such as: - SSO logins and passwords - RFA navigational support such as screens, error messages, and so on. - Mistakes made in the RFA system record such as using the wrong SAP order number or the wrong serialized hardware component in the system record. • Problems with the SAP order number or creation of the transaction record. • Downloading the FET or LIT • Problems with system records such as creating, locating, and accessing a system record.
The Avaya Services Helpdesk	The license file or the authentication file(s) such as: • Getting the license file in to the Avaya product including reading the error messages and providing solutions • FET and/or LIT interactions with DEFINITY • License-Error mode and No-License Mode • The inability to connect to DEFINITY using Connect2



Important:

If you are having trouble with the RFA application, or creating a license file or an authentication file, call the IT Helpdesk. If you need help installing a license or an authentication file, or if you are having trouble with a license or an authentication file that is already installed, call the Avaya Services Helpdesk.

[Table 3](#) shows the Helpdesk group to contact and the Helpdesk's contact information for RFA application support.

Table 3: IT Helpdesk information

Groups	Contact
● United States and Canada Avaya associates ● Members of one of the Variable Workforce Groups ● Avaya Contractors ● Avaya BusinessPartners	● For urgent matters call 866-282-2948 or (303)354-8999. ● For less urgent matters with an expected 48 hour (or more) response time send an e-mail message to userdvservices@avaya.com.
● All international callers	● No language support: 866-282-9248 or (303)345-8999 ● Language support: Contact your regional support center. Support center contact information see http://support.avaya.com/japple/css/japple?PAGE=avaya.css.OpenPage&temp.template.name=Escalations_Global

Chapter 2: Important Product Information

This chapter explains how the following product families work with RFA:

- [Advanced IP Phone Features](#) on page 21
- [Application Assurance Networking](#) on page 23
- [Application Design Environment](#) on page 25
- [Application Enablement \(AE\) Services](#) on page 27
- [Branch Gateways](#) on page 32
- [Communication Manager](#) on page 34
- [Integrated Management](#) on page 43
- [Interaction Center](#) on page 38
- [Meeting Exchange](#) on page 44
- [Modular Messaging](#) on page 45
- [Personal WorkSpace](#) on page 47
- [Security Gateway](#) on page 48
- [SIP Enablement Services](#) on page 50
- [Softclients](#) on page 52
- [Unified Communication Center](#) on page 53
- [Voice Self Service \(VSS\)](#) on page 55

Advanced IP Phone Features

Advanced IP Phone Features is a release of firmware for the Avaya 4600 series IP phone that is comprised of the Avaya IP Phone application and a VPN client. The Avaya 4600 phone uses the VPN client to establish a secure IPsec tunnel for all traffic including signalling, media and application. The use of the phone is controlled by the number of concurrent user licenses that are managed by a WebLM application residing on a WebLM server. After the VPN tunnel is established, the phone must obtain a license from the WebLM server. Once the phone obtains a license it is allowed to register with Communication Manager.

Advanced IP Phone Features license file information

[Table 4](#) shows information that you will need to know to create a license file for Advanced IP Phone Features.

Table 4: Advanced IP Phone Features license Information table

Host ID used	New Installs	Additions	Swap-Outs	RFA Feature Keyword Description	RFA Feature Keywords	Value Type
X	X	X	X	REGISTRATION is used for concurrent use of IP endpoint registration features within the server. This feature is a type 3 feature and will have a quantity associated with it. If the feature setting is MAX than the setting for this feature is at its allowed maximum.	REGISTRATION	3
				FEAT_ENTERPRISE activates the enterprise licensing on the WebLM server. This feature is a type 1 feature with a on or off setting. When this feature is set to 'ON', the WebLM server acts as the master WebLM server. A master WebLM server is used for administration of local WebLM servers and can be used to generate allocation license files for enterprise licensing.	FEAT_ENTERPRISE	1

Application Assurance Networking

Application Assurance Networking is a Linux-based application that runs on specific configurations of IBM eServer xSeries 306 and 336 platforms. Application Assurance Networking performs the following functions:

- Identifies the applications running on the network.
- Monitors the quality of service (QoS) provided by the network to each application session over a specific network path.
- Determines an alternate network path providing a greater QoS.
- In real-time, reroutes application sessions to better performing paths, without the applications or the users being aware of the reroute.

Currently there is only one application under the Application Assurance Networking product family that is licensed by RFA.

Application Assurance Networking license file information

[Table 5](#) shows information that you will need to know to create a license file for Application Assurance Networking.

Table 5: Application Assurance Networking license file information table

Host ID used	New Installs	Additions	PCN Updates	Upgrades	Swap-Outs	RFA Feature Keyword Description	RFA Feature Keywords	Value Type
X	X	X	X	X	X	Reporting Only mode enabled, web application model	VALUE_AAN_CNA	2
						Web application reporting only tier	VALUE_AAN_CNA_TIER	2
1 of 2								

Table 5: Application Assurance Networking license file information table (continued)

Host ID used	New Installs	Additions	PCN Updates	Upgrades	Swap-Outs	RFA Feature Keyword Description	RFA Feature Keywords	Value Type
						Route Assert mode enabled	VALUE_AAN_APC	2
						Route Assert tier	VALUE_AAN_APC_TIER	2
						VoIP application model configurable	VALUE_AAN_VOIP	2
						VoIP tier	VALUE_AAN_VOIP_TIER	2
						Enterprise application model configurable	VALUE_AAN_ENT	2
						Enterprise tier	VALUE_AAN_ENT_TIER	2
						Real-time multimedia app model configurable	VALUE_AAN_MMED	2
						Multimedia tier	VALUE_AAN_MMED_TIER	2
						Streaming audio and video app model configurable	VALUE_AANSTRM	2
						Streaming audio and video tier	VALUE_AANSTRM_TIER	2
						Load table entries enabled	VALUE_AAN_WCO	2
						Load table entries tier	VALUE_AAN_WCO_TIER	2
2 of 2								

Application Design Environment

Application Design Environment (ADE) is the product family name within RFA. Dialog Designer (DD) is the only application under the ADE product family that requires an RFA license.

There are two major components of DD:

- A development environment that runs on a PC.
- A run-time component that runs on a web container on a web server.

The run-time component is the only component of DD that is licensed in RFA.



Important:

When the Dialog Designer CTI Connector is used through the Application Enablement Services JTAPI/TSAPI interface, the appropriate number of Application Enablement VALUE_TSAPI_USERS must be set. This setting may cause a change in the Application Enablement product family license. The correct number of VALUE_TSAPI_USERS that you enable is based on the number of supported VRU channels that use CTI simultaneously.

RFA licensed ADE components

[Table 6](#) shows a list of what is being licensed by RFA for ADE.

Table 6: ADE licensed components

Product family application description	Application name in RFA	What is being licensed?
ADE	Dialog Designer	• The Dialog Designer standalone package • The Computer Telephony Integration (CTI) library enablement • The Computer Telephony Integration (CTI) library universal enablement • The IC library enablement • The IC library universal enablement

ADE license file information

[Table 7](#) shows that you will need to know to create a license file for ADE.

Table 7: Application Design Environment license file information table

Host ID used	New Installs	Additions	PCN Update	Upgrade	Swap-Out	RFA Feature Keyword Description	RFA Feature Keywords	Value Type
X	X	X	X	X	X	DD standalone package: Allows customers without an Avaya IR or VP platform to run Dialog Designer applications.	VALUE_DD_UNIVERSAL	2
						CTI library enablement: Allows Avaya IR/VP customers who have purchased the CTI connector to interface with the CTI server through Dialog Designer applications.	VALUE_DD_CTI_LIBRARY	2
						CTI library universal enablement: Allows customers who don't have an IR/VP platform, but do have an Avaya CTI system to use the CTI connector in Dialog Designer to interface with their CTI system(s).	VALUE_DD_CTI_LIBRARY_UNIVERSAL	2
1 of 2								

Table 7: Application Design Environment license file information table (continued)

Host ID used	New Installs	Additions	PCN Update	Upgrade	Swap-Out	RFA Feature Keyword Description	RFA Feature Keywords	Value Type
						IC library enablement: Allows Avaya IR/VP customers who have purchased the IC connector to interface with their IC system through Dialog Designer applications.	VALUE_DD_IC_LIBRARY	2
						IC library universal enablement: Allows customers who don't have an IR/VP system, but who have an Avaya IC system, to use the IC connector in Dialog Designer to interface with their IC system(s).	VALUE_DD_IC_LIBRARY_UNIVERSAL	2
2 of 2								

Application Enablement (AE) Services



Important:

CVLAN is called Application Enablement (CTI) in RFA. Application Enablement (CTI) is the new name in RFA for the products formerly known as Computer Telephony Integration (CTI).

Upgrading to AE

You can upgrade to AE from a:

- Non-RFA windows platform (Avaya CT)
- CVLAN R9
- DEFINITY LAN Gateway (DLG):
 - Upgrades from DLG co-resident on Communication Manager to AE are supported.
 - Upgrades from a MAPD board to DLG are not supported.

An Upgrade to AE is considered a new install. You must invoke the new install functionality in RFA to perform the upgrade.

Upgrading CVLAN R9 to AE

Use the following process to upgrade CVLAN R9 to AE:

1. Obtain the existing System Identification Number (SID) of the CVLAN R9 to be upgraded to AE.
2. Call the help desk.
3. The help desk:
 - Checks the SID to verify that the RFA record is assigned to a CVLAN R9.
 - Executes the AE Conversion script that converts the CVLAN R9 system record to an AE system record.

Upgrading DEFINITY LAN Gateway to AE

DEFINITY LAN Gateway (DLG) can be installed on a MAPD board or co-resident on the same server as Communication Manager. When DLG is co-resident with Communication Manager, an upgrade to AE is considered a new install in RFA. There is no upgrade path to AE for a DLG on a MAPD board.

Note:

Communication Manager Release 3.0 does not support co-resident DLG.

CVLAN Server 9.0 for Linux

CVLAN is an Application Programming Interface (API) that allows applications to communicate with Avaya Communication Manager. The communication path between the CVLAN server and the Communication Manager server is made up of one or more ASAI links.

The CVLAN operating environment includes the following:

- CVLAN client
- CVLAN server running Linux 9.0
- Communication Manager server

CVLAN Client: The CVLAN client software runs on a workstation or a server and provides access to the Communication Manager server by way of the CVLAN server. You can obtain the CVLAN client software from the Avaya web site. You do not need an RFA license file for the CVLAN client software. Refer to Avaya CVLAN Server for 9.0 Linux Installation and Basic Administration Guide for information on the downloading the CVLAN client software.

CVLAN server: The CVLAN server software runs on a Linux based PC and manages ASAI traffic between the Communication Manager server and the CVLAN client. The CVLAN server requires an RFA license file.

RFA licensed AE applications

[Table 8](#) shows what is being licensed for the applications that are in the AE product family.

Table 8: AE applications license information

Product family application description	Application name in RFA	What is being licensed
MVAP Server	Application Enablement Connections	Number of connections
CallVisor LAN	CVLAN	● Application ● Number of connections ● Proprietary links
DEFINITY LAN Gateway	DLG	Application
Telephony Services API	TSAPI	● Application ● Number of users ● Number of advanced users

AE license file information

[Table 9](#) shows information that you will need to know to create a license file for AE.

Table 9: AE license file information table

Host ID	Host ID information	New Installs/Migrations	Additions	Swap-Out	RFA Feature Keyword Descriptions	RFA Feature Keywords for AE	Value Type
X	For AE the Host ID is the Media Access Control Address (MAC) of the first ethernet port (eth0) on the server.	X	X	X	Application Enablement Connections Version	VALUE_AEC_VERSION	2
							1 of 2

Table 9: AE license file information table (continued)

Host ID	Host ID information	New Installs/Migrations	Additions	Swap-Out	RFA Feature Keyword Descriptions	RFA Feature Keywords for AE	Value Type
					Application Enablement Connections	VALUE_AEC_CONNECTIONS	2
					CVLAN	VALUE_CVLAN	2
					CVLAN Version	VALUE_CVLAN_VERSION	2
					CVLAN Proprietary Links	VALUE_PROPRIETARY_LINKS	2
					CVLAN Switch Connections	VALUE_SWITCH_CONNECTIONS	2
					DLG	VALUE_DLG	2
					TSAPI Version	VALUE_TSAPI_VERSION	2
					TSAPI Simultaneous Users	VALUE_TSAPI_USERS	2
					TSAPI Simultaneous Advanced Users	VALUE_TSAPI_ADVANCED_USERS	2
2 of 2							

Branch Gateways

The G250 and the G350 media gateways are the only RFA supported gateways in the Branch Gateways product family. License file requirements for the G250 and the G350 media gateway vary depending on the configuration.

Use the information in [Table 10](#) to determine when an RFA license file is needed.

Table 10: Branch Gateways information table

G250/G350 Configuration	RFA license required?
A Standalone G250 or a G350 without Virtual Private Networking (VPN).	No.
A standalone G250 or a G350 with VPN.	Yes. You need one RFA license file to activate VPN.
A standalone G250 or G350 with an S8300 Media Server.	Yes. You need one RFA license file for Communication Manager.
A standalone G250 or G350 is with an S8300 Media Server and VPN.	Yes. You need two RFA license files: ● One for Communication Manger ● One to activate the VPN feature
The G250 or G350 is remotely controlled by a server. The G250 or G350 does not have VPN.	No.
The G250 or the G350 is remotely controlled by a server. The G250 or the G350 has an S8300 Media Server acting as an LSP.	Yes. You need one RFA license file for the LSP.
The G250 or the G350 is remotely controlled by a server. The G250 or the G350 has an S8300 Media Server acting as an LSP and has VPN.	Yes. You need two RFA license files: ● 1 for the LSP ● 1 for the VPN

The serial number for the G250 or G350 Media Gateway

Each Branch Gateway has a license file that contains a unique serial number. The same serial number cannot be used more than once within the Branch Gateways product family. When the G250 or the G350 has VPN and a S8300 Media Server, you need two license files. In this case, the serial number of the G250 or the G350 can be used for both license files because each license file is created in a different product group. In this example, the G250 or the G350 with VPN is licensed in the Branch Gateway product family while the S8300 Media Server is licensed in the Communication Manager product family.

To identify the G250 or the G350 serial number type, `show sys` from the command line interface.

Post installation verification

If you attempt to load a license file with a serial number that does not match the serial number of the new G250 or the G350 media gateway:

- The license file fails to install
- A SNMP notification is sent
- A message is written in the Syslog

Activating the VPN

After you load the license file, you must perform a reset on the G250 or the G350 media gateway to activate VPN. A feature setting of 1 indicates that VPN is turned on. A feature setting of 0 (zero) indicates VPN is turned off.

Branch Gateway license file information

[Table 11](#) shows information that you will need to know to create a license file.

Table 11: Branch Gateway license file information table

New Installs/Migrations	Additions	Swap-Out	RFA Feature Keyword Descriptions	RFA Feature Keywords	Value Type
X	X	X	Virtual Private Networking	VALUE_VPN	2
			Platform	VALUE_PLATFORM	2

Communication Manager

A separate license file is required for each of the following Avaya servers:

- DEFINITY Server R, SI, and CSI (starting with release 10)
- DEFINITY ONE or IP600 (starting with release 10)
- Media servers:
 - S8100
 - S8300
 - S8500
 - S8700 series servers
- WAN Spare Processor (WSP)
- Survivable Remote Processor (SRP)
- Local Survivable Processor (LSP)
- Enterprise Survivable Server (ESS)

Note:

An Avaya system that is equipped with a duplicated processor only requires one license file. This license file contains the serial number for both processors.

Communication Manager requires a license file when you are performing one of the following:

- An installation or a migration
- An addition
- A PCN update
- An upgrade
- A server or processor swap-out

A list of Feature Keywords and Feature Keyword descriptions can be found in the *DEFINITY/MultiVantage/Avaya Communication Manager and Audix Feature Keywords* document at <http://rfa.avaya.com>.

Serial numbers for Communication Manager

You can find the serial number for Communication Manager in one of the following ways:

- Hardware: All Communication Manager servers and IPSI boards have the serial number printed on a label found in the front or the back of the hardware.
- Firmware: Serial numbers can also be identified through the firmware of the server or IPSI board.
- RFA (DEFINITY only): RFA provides a method to retrieve serial numbers on Avaya DEFINITY servers.

For more information on how to find the serial number for a Communication Manager server, see *The Remote Feature Activation (RFA) User Guide* at <http://support.avaya.com>.

Working with authentication files

In addition to the license file, Avaya servers that use an open operating system require an authentication file. The authentication file contains non-default passwords and Access Security Gateway (ASG) keys for the Avaya services logins. When you create an RFA system record for an Avaya system Release 11 and later, RFA automatically creates an authentication file.

Note:

The Avaya DEFINITY servers do not run on an open operating system and therefore do not require an authentication file.

Note:

For the S8100 Media Server Release 10 or earlier, the Automatic Registration Tool (ART) is used to generate the authentication file. ART is available to Avaya associates or the regional registration teams.



CAUTION:

If you are going to request a new authentication file, you must be logged in to the server before you request the new ASG key. If you are not logged in to server you will be locked out and will not have access to the server.

DEFINITY upgrades

DEFINITY upgrades may consist of one of the following:

- An upgrade:
 - From a DEFINITY Release 4 to a DEFINITY Release 9
 - From a DEFINITY release to a Communication Manager release
- A DEFINITY server that is upgrading within the same platform. Platforms for DEFINITY include the CSI, the SI, the R, the DEFINITY ONE, and the IP600.

Note:

The Feature Extraction Tool (FET) must be used to extract features from a DEFINITY server that is upgrading to Release 10 or later. For more information on FET, see *The Remote Feature Activation (RFA) User Guide* at <http://support.avaya.com>.

DEFINITY migrations

A DEFINITY migration may consist of one of the following:

- DEFINITY ONE to S8700 IP Connect
- DEFINITY ONE to DEFINITY CSI
- DEFINITY ONE to DEFINITY SI
- DEFINITY G3i, s, or vs, to DEFINITY CSI
- DEFINITY G3i, si, or vs, to DEFINITY SI
- DEFINITY G3d, G3i, or G3si, to DEFINITY R
- DEFINITY G3s, G3i, or G3si, to S8700 Multi-Connect
- DEFINITY R to S8700 Multi-Connect
- Any system that is currently at pre Version 4 upgrading to a Communication Manager release
- Upgrades from pre Release 4 to a Release 10

Note:

DEFINITY migrations cannot use FET to extract existing features. Instead the GES configurator provides tracking or migration codes that carry forward optional features and capacities previously purchased to the new system record and license file. When the account team requests a DEFINITY migration in the GES configurator, they manually identify and input the existing features. The configurator produces an output containing both existing features and new capabilities on a single SAP order.

The Shared Blade Server

The Shared Blade Server (SBS3000) system uses virtual machines plus multiple blades to allow multiple instances of Communication Manager on one SBS3000 system. RFA contains a system record for each instance of Communication Manager running on an SBS3000 system. Each system record is populated based on the specific instance of Communication Manager. RFA is also used to generate additional licenses over the life of the system to support maintenance activities such as an IPSI or gateway replacement. Communication Manager software sets the license mode accordingly at system initialization and checks the license file at installation and periodically thereafter.

Note:

RFA is not used to for registration to Avaya. You must manually register the SBS3000 and the associated applications that run on the SBS3000's virtual machines.

For Communication Manager, RFA defaults to using CLAN registration to download a license file. If an alternate PCLAN configuration is used, the changes outlined in [Table 12](#) are required.

Table 12: SBS licensing information

	Licensed Object	FEAT_IP_PNC	FEAT_PNS	FEAT_PRETH	LSP
SBS3000: Communication Manager in CLAN mode (default)	Reference ISPI	Off	On	Off	Off
1 of 2					

Table 12: SBS licensing information (continued)

	Licensed Object	FEAT_IP_PNC	FEAT_PNS	FEAT_PRETH	LSP
SBS3000: Communication Manager in PCLAN mode	Serial number of the H.248 gateway	Off	Off	On	Off
SBS3000B: LSP	Serial number of H.248 gateway	Off	Off	On	On
					2 of 2

Interaction Center

RFA is used to obtain a license file for Interaction Center (IC) when:

- IC is purchased with Release 6.1.3 or later.

Note:

When IC is purchased with Release 6.1.3 or later, the Interaction Center Operational Analyst (IC/OA) Price Tool version 3.4 or later is required.

- IC is used in a production environment. If IC is being used for demonstration or evaluating purposes, an RFA license is not needed.
- A single WebLM (one Host ID) environment is being used.
- A permanent license is needed.
- A change in the Host ID is needed. In this case the RFA Swap-Out functionality is used to create a new license file containing the new Host ID.

Note:

If your Avaya IC system includes multiple sites, or a redundant multi-server solution, you need a series of segmented licenses. Each segmented license is specific to a WebLM application in your Avaya IC system. In these situations, RFA is not used to generate a license file. When RFA is not used to license IC, the E-mail License Request process at icoakeyrequest@avaya.com is used.

E-mail license request and IC

Use the existing E-mail License Request process when:

- IC is being used in a non-production environment. In this case IC uses a development and test license.
- IC was purchased with release 6.0.X through 6.1.2, or you are upgrading IC from a earlier release.
- Multiple WebLM applications are used requiring multiple segmented licenses.
- The customer is evaluating IC.
- IC contains a temporary license.

Note:

An Operational Analyst (OA) license can be requested by the E-mail License Request process.

IC license file information

[Table 13](#) shows information that you need to know to create a license file for IC.

Table 13: Interaction Center license file information table

Host ID	Host ID information	New Installs/Migrations	Additions	PCN Update	Upgrade	Swap-Out	RFA Feature Keyword Description	RFA Feature Keywords	Value Type
X	The Host ID is the Media Access Control Address (MAC) of the first ethernet port (eth0) on the server.	X	X	X	X	X	Max num users concurrently logged into IC Max num users for inbound voice channel media	VALUE_TOTALAGENTS VALUE_INBOUNDVOICE AGENTS	2 2
							Max num users for email media channel Max num users for web media channel	VALUE_EMAILAGENTS VALUE_WEB AGENTS	2 2
1 of 3									

Table 13: Interaction Center license file information table (continued)

Host ID	Host ID information	New Installs/Migrations	Additions	PCN Update	Upgrade	Swap-Out	RFA Feature Keyword Description	RFA Feature Keywords	Value Type
							PeopleSoft connector enabled	FEAT_PEOPLESFT SERVER	1
							Sibel 7 Connector enabled	FEAT_SIBLE7GW	1
							Sibel 2000 Connector enabled	FEAT_SIBLE2000GW	1
							Max num of content analysis servers	VALUE_CONTENT ANALYSISVRS	2
							Business Advocate feature enabled	FEAT_BUSINESS ADVOCATE	1
							Max num Softdialer agents	VALUE_SOFT DIALERSVRS	2
							Max num Softdialer servers	VALUE_SOFT DIALERSVRS	2
2 of 3									

Table 13: Interaction Center license file information table (continued)

Host ID	Host ID information	New Installs/Migrations	Additions	PCN Update	Upgrade	Swap-Out	RFA Feature Keyword Description	RFA Feature Keywords	Value Type
							Outbound feature of import list enabled	FEAT_SOFT DIALERIMPORT LIST	1
							Outbound feature of predictive dialing enabled	FEAT_SOFT DIALER PREDICTIVE	1
							Max num Avaya switch servers	VALUE_TS DEFINITYSVRS	2
							Max num Aspect switch servers	VALUE_TS ASPECTSVRS	2
							Max num Nortel Meridian switch servers	VALUE_TS MERIDIAN	2
							Max num Nortel Symposium switch servers	VALUE_TS SYMPOSIUM SVRS	2
									3 of 3

Integrated Management

RFA supports the following application within the Integrated Management product family:

- VoIP Monitoring Manager (VMM): An RFA license file is required for VoIP Monitoring Manager 3.0 or later. VMM versions earlier than 3.0 do not require an RFA license file.

Refer to [Table 14](#) for information on applications licensed by RFA for Integrated Management.

Table 14: Integrated Management applications

¹ RFA Application Name for Integrated Management	What is being licensed
Integrated Management Monitoring Solutions	● Application (3.0 or later) ● Number of endpoints: - Up to 2000 - Additional 2000 ● Gateways: - Up to 40 - Additional 40

¹ The RFA Application Name is the name that represents Integrated Management within RFA.

On new installations of Integrated Management, an SAP order is used to enable the minimum quantities for both endpoints and gateway capacity. The RFA New Install capability is used to create a system record and generate a license file.

For additional endpoint and gateway capacity, a SAP order is required. Endpoints and gateways are bundled together in quantities of 2,000 endpoints and 40 gateways. The RFA Additions capability is used to add the new capacity and generate a new license file.

Integrated Management license file information

[Table 15](#) shows information that you need to know to create a license file for Integrated Management.

Table 15: Integrated Management license file information table

Host ID	Host ID information	New Installs/Migrations	Additions	PCN Update	Upgrade	Swap-Out	RFA Feature Keyword Description	RFA Feature Keywords	Value Type
X	For Integrated Management, a Host ID is the Media Access Control Address (MAC) of the first ethernet port (eth0) on the WebLM server	X	X	X	X	X	VoIP Monitoring Manager (VMM) Version Maximum Number of Endpoints Maximum Number of Gateways	VALUE_VMM_VERSION VALUE_VMM_ENDPOINT VALUE_VMM_GATEWAY	2 2 2

Note:

The number of gateways and the number of endpoints are calculated separately. Additional quantities must be purchased if a customer exceeds **either** the maximum purchased endpoints or managed gateways.

Meeting Exchange

Meeting Exchange Groupware Edition is shipped pre-configured to the customer. The assembly and test team is responsible to obtain the license file from RFA and load the license on to the Meeting Exchange server.

A unique Host ID is required to license each instance of Meeting Exchange. For help in finding the Host ID on your Meeting Exchange server, see the *Avaya Remote Feature Activation (RFA) User Guide* located at <http://support.avaya.com>.

RFA supports the following application within the Meeting Exchange product family:

- Groupware Edition

Meeting Exchange license file information

[Table 16](#) shows information that you need to know to create a license file for Meeting Exchange.

Table 16: Meeting Exchange license file information table

Host ID	Host ID information	New Installs/Migrations	Additions	PCN Update	Upgrade	Swap-Out	RFA Feature Keyword Description	RFA Feature Keywords	Value Type
X	For Meeting Exchange, the Host ID is the Media Access Control Address (MAC) of the first ethernet port (eth0) on the Meeting Exchange server.	X	X	X	X	X	Number of Meeting Exchange Groupware Edition G.711 CODEX supported.	VALUE_MXGE_G711_CODEX	2
							Number of Meeting Exchange Groupware Edition ports.	VALUE_MXGE_PORTS	2

Modular Messaging

An RFA license is required for the following Modular Messaging features:

- Seats: The number of voice mail-enabled mailboxes that are being licensed.
- Text-to-Speech/engine type/language: The number and type of concurrent sessions of test-to-speech conversion that is being licensed.
- Platform: Messaging platform that is being licensed. Different versions of Modular Messaging work with Avaya, Microsoft, and IBM/Lotus messaging stores.

Host ID information

For Modular Messaging the Host ID is the voice mail domain identifier. The Host ID may be alpha/numeric and can be up to 50 characters in length. The format for a Modular Messaging Host ID is:

<8 hex char>-<4 hex char>-<4 hex char>-<4hex char>-<12 hex char>

Note:

Modular Messaging does not distinguish between upper and lower case letters.

Note:

For information on how to find the Host ID for Modular Messaging, see *The Remote Feature Activation (RFA) User Guide* at <http://support.avaya.com>.

Post installation verification

If the Host ID in the RFA license file does not match the Host ID in the Modular Messaging system, the License import Wizard in VMSC fails. The system displays a message that states that the license is not valid. The Windows event log on MAS, through which the import was requested, also contains an error event that says "The license does not refer to this system. Please obtain a new license."

Modular Messaging license information

[Table 17](#) shows information that you need to know to create a license file for Modular Messaging.

Table 17: Modular Messaging license file information table

Host ID	Host ID information	New Installs/Migrations	Additions	PCN Update	Upgrade	Swap-Out	RFA Feature Keyword Description	RFA Feature Keywords	Value Type
X	Modular Messaging Host IDs are known as voice mail domain identifier outside of RFA.	X	X	x	X	X	Platform	VALUE_PLATFORM	2
							Modular Messaging Mailboxes	VALUE_MM_SEATS	2
							Text to speech, ScanSoft RealSpeak, Any Language	VALUE_TTS_REALSPEAK_ANY	2
							Text to speech, Fonix, DECTalk US English	VALUE_TTS_DECTALK_EN_US	2
							Text to speech, Scansoft TTS-3000 International	VALUE_TTS_TTS3000_INT	2

Personal WorkSpace

Personal WorkSpace (PWS) phase 1 is a client-server based software solution that allows the user to access personal telecommunications and services through end-user interfaces. An RFA license file is required on each server that hosts the PWS application. Each PWS server can support up to 1000 clients per server. Multiple PWS servers may be required as additional capacity is needed.

PWS licensing information

[Table 18](#) shows information that you need to know to create a license file for PWS.

Table 18: Personal WorkSpace license file information table

Host ID used	New Installs	Upgrades	PCN Updates	Additions	Swap-Out	RFA Feature Keyword Descriptions	RFA Feature Keywords	Value Type
X	X	X	X	X	X	Maximum number of administered users	VALUE_PWS_USER	2

Security Gateway

Avaya ships the Security Gateway product family with a default license file. An Avaya Security Gateway does not require an RFA license file unless additional capabilities are added. Additional capabilities include increasing the number of site-to-site connections and remote users.

Since the Security Gateway unit is shipped with a default license file the Security Gateway does not have a corresponding system record in RFA. When you add additional capabilities for the first time, use the New Install option in the RFA Application Main Menu. After the system record is created in RFA, use the RFA Additions functionality to create any future license files.

When you create a license file, the RFA system record reflects only the additional capabilities contained in the SAP order. RFA does not reflect the default settings. You can use the RFA **Features** screen to view the additional capacities. The Security Gateway combines both the capabilities of the default settings and the capabilities in the license file. [Table 19](#) shows an example of a Security Gateway with increased capabilities.

Table 19: Security Gateway example

Scenario	Site-to-Site Connections	Remote Users
The default settings of the Security Gateway	25	50
The additional capabilities from the SAP order	10	30
RFA system record reflects this total	10	30
Security Gateway provides this total capability	35	80

Security Gateway models

Avaya requires a RFA license file on the following Security Gateway Solutions models:

- SG5 Security Gateway
- SG5X Security Gateway
- SG200 Security Gateway
- SG203 Security Gateway
- SG208 Security Gateway

Note:

An RFA license is not required for Security Gateway unless you are adding additional site-to-site connections or remote users that are above the default entitlements.

Security Gateway license file information

[Table 20](#) shows information that you need to know to create a license file for Security Gateway.

Table 20: Security Gateway license file information

Serial Number	New Installs/Migrations	Additions	Swap-Out	RFA Feature Keyword Description	RFA Feature Keywords	Value Type
X	X	X	X	Site-to-site Remote Users	VALUE_SITETOSITE	2
				Number of Remote Users	VALUE_REMOTEUSERS	2

SIP Enablement Services

SIP Enablement Services integrates with Communication Manager to extend a set of SIP-based software services and SIP registration for:

- All current endpoints
- SIP endpoints
- Third-party applications

Most often, the SIP Enablement Services application requires SIP Trunking activated on the host Communication Manager server. Avaya Communication Manager, Release 2.0 and later, integrates with SIP Enablement Services as a telephony feature server to SIP-based endpoints.

The SIP Enablement Services solution typically requires two RFA license files: One for the Communication Manager host server, to activate SIP trunking, and one for the SIP Enablement Services server.

SIP Enablement Services module type

There is a single module type for SIP Enablement Services. The module type for SIP Enablement Services is SES_Main.

Post installation verification

If the Host ID of the server and the Host ID within the license file do not match, the SIP Enablement Services server enters in to a license-error mode. The SIP Enablement Services server can run in a license-error mode for up to 10 days. Service is not affected while the server is in the license-error mode. If the problem that created the license-error mode is not corrected after the 10 days, the SIP Enablement Services server ceases to operate.

SIP Enablement Services license file information

[Table 21](#) shows information that you need to know to create a license file for SIP Enablement Services.

Table 21: SIP Enablement Services license file information

Host ID	Host ID information	New Installs/Migrations	Additions	PCN Update	Upgrade	Swap-Out	RFA Feature Keyword Description	RFA Feature Keywords	Value Type
X	For SIP Enablement Services, a Host ID is the Media Access Control Address (MAC) of the first ethernet port (eth0) on the server.	X	X	X	X	X	Number of Edge Proxy seats Number of Basic Proxy seats Number of Client seats	VALUE_EDGE_PROXY VALUE_BASIC_PROXY VALUE_CLIENTS	2 2 2

Softclients

The Softclients product family contains one RFA licensed application that is named SIP Softphone.

Over a SIP, the Avaya SIP Softphone is a PC-based endpoint enabling users to:

- Initiate and receive calls
- Send and receive instant messages

There are three supported SIP softphone configurations:

- Avaya SIP Infrastructure (Converged Communications Server): When the Avaya SIP Softphone operates in a CCS environment, the SIP Softphone communicates using TLS with Avaya CCS 2.x and later. The SIP Softphone implements features as per IETF RFC 3261, IETF drafts for message-waiting indication, and a subset of the SIPPING 19 features (where applicable). For more information on CCS see [SIP Enablement Services](#) on page 50.
- Non-Avaya SIP Proxy, registrar, and endpoints: When the Avaya SIP Softphone operates in a non-Avaya SIP Proxy environment, it communicates using TCP and UDP with other vendor's SIP proxies, registrar, and endpoints. The SIP Softphone implements the SIPPING 19 (where applicable).
- No SIP Infrastructure (Peer-to-Peer): When the Avaya SIP Softphone is installed in an environment where no proxies are used, SIP Softphone provides basic telephony and IM functionality when communicating directly with another Avaya SIP Softphone.

Softclients Host ID information

The Host ID that is used for Softclients is the MAC address of the first Network Interface Card (NIC) on the WebLM server. The Host ID may consist of:

- Numbers and letters
- Up to 50 characters in length
- Upper and lower case letters
- Some special characters

Softclients license file information

A license for SIP Softphone contains the maximum number of SIP Softphones that can be running at one time. Once the maximum number is obtained, a user attempting to start a new session receives an error message that directs them to contact their support organization.

There is a single module type for Softclients. The name for the module type is SIPSP_Main.

[Table 22](#) shows information that you need to know to create a license file for Softclients.

Table 22: Softclients license file information table

Host ID	New Installs/Migrations	Additions	Swap-Out	RFA Keyword Description	RFA Keywords	Value Type
X	X	X	X	IP Endpoint Registration	REGISTRATION	3

Unified Communication Center

Unified Communication Center (UCC) consists of a suite of applications. Each application uses the UCC License Server to obtain a license that allows the UCC application to run. The UCC applications are:

- Avaya Web Messaging Application (WMA)
- Avaya Web Collaboration Application (WCA)
- Avaya Advanced Speech Access (ASA)

A UCC License Server software is a product called Avaya License Manager. The RFA license file is installed on the UCC License Server. If the customer purchases the Web Messaging Application (WMA) or the Web Collaboration Application (WCA), then the UCC License Server is the UCC Base Server. If the customer purchases only the Advanced Speech Access (ASA) application, then the UCC License Server is the ASA Server (UCC Speech Server).

The UCC license file contains feature settings for the following:

- For the Web Messaging and Web Collaboration applications:
 - Number of seats: The number of people who can use each UCC application at the same time.
 - Expiration date

Important Product Information

- For the Advanced Speech Access application:
 - Number of seats
 - Expiration date
 - Number of Automatic Speech Recognition ports
 - Number of Text-to-Speech sessions

UCC Host ID information

For UCC the Host ID is the MAC address of the first Network Interface card in the UCC license server. If the customer purchases the:

- Web Messaging Application (WMA) or the Web Collaboration Application (WCA), the Host ID is the MAC address of the first Network Interface Card (NIC) in the UCC Base Server.
- Advanced Speech Access (ASA) application only, the Host ID is the MAC address of the first NIC in the ASA Server. The ASA server is also referred to as the UCC Speech Server.

UCC license file information

[Table 23](#) show information that you need to know to create a UCC license file.

Table 23: UCC license file information table

New Installs/Migrations	Additions	Upgrade	Swap-Out	RFA Keyword Description	RFA Keywords	Value Type
X	X	X	X	Number of Adv. speech resource ports	VALUE_ASR_PORTS	2
				Number of Text to Speech ports	VALUE_TTSPTS	2
				Number of seats	VALUE_SEATS	2
				Number of switch connections	VALUE_SWITCH_CONNECTIONS	2
				Text to speech, ScanSoft RealSpeak, any language	VALUE_TTS_REALSPEAK_ANY	2
				Maximum ports	VALUE_PORT	2
				Node locking	FEAT_NODELOCK	1

Voice Self Service (VSS)

The Voice Self Service (VSS) product family contains two applications that require an RFA license file:

- Interactive Response
- Voice Portal

VSS Host ID information

VSS uses the MAC address of the first Network Interface Card (NIC) on the WebLM server for licensing. The Host ID can contain:

- Numbers or letters
- Up to 50 characters in length
- Upper and lower case letters
- Some special characters

VSS license file information

[Table 24](#) shows information that you need to know to create a license file for VSS.

Table 24: VSS license file information table

Host ID used	New Installs	Additions	Upgrades	PCN Update	Swap-Out	RFA Keyword Description	RFA Keywords	Value Type
X	X	X	X	X	X	This Feature Keyword enables the Enterprise Licensing feature on the WebLM server	FEAT_ENTERPRISE	1
1 of 2								

Table 24: VSS license file information table (continued)

Host ID used	New Installs	Additions	Upgrades	PCN Update	Swap-Out	RFA Keyword Description	RFA Keywords	Value Type
						Number of IR ports	VALUE_IR_PORTS	2
						Number of ASR ports	VALUE_IR_ASR_PORTS	2
						Number of Test to Speech ports	VALUE_IR_TTS_PORTS	2
						Number of servers with SNMP enabled	VALUE_IR_SNMP	2
						Maximum number of concurrent telephony ports	VALUE_VP_PORTS	2
						Maximum number of ASR connections	VALUE_VP_ASR_CONNECTIONS	2
2 of 2								

Glossary

F

Feature Keywords	See Feature Keywords on page 16. RFA uses Feature Keywords to identify features
FSO	Field Service Organization

G

GAI	See Group Authorization Identification (GAI) on page 16.
------------	--

L

License File	Encrypted file that activates features and capacities
---------------------	---

P

PCN	Product Correction Notice (formally known as QPPCN).
POST	Avaya's internal directory web resource.
Product family	Identifies the Avaya product line such as Avaya Communication Manager and Branch Gateways.

R

RFA	Remote Feature Activation. See Chapter 1: Remote Feature Activation Overview on page 13.
RFA IBM Helpdesk	Navigational, escalation and SSO password support for the RFA application.
RTU	Right-to-use

S

SAP	Avaya's ordering system for products and services.
Serial numbers	A serial number of the Avaya hardware is used to create a valid license file. The hardware serial number and the serial number within the license file must match.
Swap-Out	RFA functionality used to create a new license file for maintenance.
SSO	Single Sign-On is the Avaya corporate mechanism requiring a single login to allow users access to certain web sites.
System Record	An RFA record for each licensed Avaya product.

Tier I BusinessPartner

T

Tier I BusinessPartner A BusinessPartner that has a direct purchasing relationship with Avaya (Distributor).

Tier II BusinessPartner A BusinessPartner that purchases from a Tier I BusinessPartner (Dealer).

Transaction Record Temporary state when an RFA System Record is being created or updated. This converts to a permanent System Record upon completion.

Type 2 features A feature that has a value.

Index

A

Advanced IP Phone Features	21
license file information	22
AE	27
Applications	29
CVLAN Server 9.0 for Linux	29
CVLAN Client	29
CVLAN server	29
License file information	30
Upgrading CVLAN R9 to AE	28
Upgrading DLG to AE	28
Upgrading to	28
Application Assurance Networking	23
License file information	23
Application Design Environment	
Components	25
License file information	26
Application Design Environment (ADE)	25
Application Enablement Services	27
Application readiness checklist	18
Authenticated	13
Authentication file	35
Authentication files	36
Availability	14
Avaya support center	17

B

Branch Gateways	32
License file information	34

C

Communication Manager	34
Authentication file	35
Computer requirements	13
conventions	8

D

DEFINITY	
Migrations	36
Upgrades	36
Design Configuration	14
downloading this book	8
downloading updates from the Web	8

F

Feature Keywords	16
----------------------------	--------------------

G

G250 and G350	
Activating Virtual Private Networking	33
Activating VPN	33
Post installation verification	33
Remotely controlled by a server	32
Remotely controlled by a server with an LSP	32
Remotely controlled by a server with an LSP and VPN	32
With an S3800 and VPN	32
With an S8300	32
G250 and G350 serial number	33
G250 Media Gateway	32
Configurations	32
G350 Media Gateway	32
Configurations	32
Standalone G350 with VPN	32
Standalone G350 without VPN	32
GAI	15 , 16
Group Authorization Identification	15

H

Help for RFA	19
Help information	17
Host IDs	17
HRID	13

I

Important product Information	21
Integrated Management (Avaya IM)	43
License file information	43
Interaction Center	38
Email license request	39
License file information	40

M

Material Codes	16
Meeting Exchange	44
License file information	45
Migrations	36

Index

Modular Messaging	45
Host IDs	46
License file information	46
Post installation verification	46

P

Personal WorkSpace.	47
Licensing information	48
Pre-installation check list	18

R

Registered	13
Registration for Avaya Associates.	14
Registration for Avaya BusinessPartners	15
Reliability	14
RFA	
Access.	13
Overview.	13

S

S8300 Media Server	
Acting as an LSP	32
Acting as an LSP with VPN	32
Standalone G250 and G350 with an S8300.	32
Standalone G250 or G350 with an S8300 and a VPN	32
SBS3000	37
Security Gateway	48
Security Gateways	
License file information	50
Models.	49
Serial numbers	17
Communication Manager	35
Firmware	35
Hardware	35
Shared Blade Server.	37
SIP Enablement Services	50
License file information	51
Post installation verification	51
Softclients	52
CCS	52
Host ID information	52
License file information	52
Peer-to-Peer	52
SIP Softphone	52
Swap-Out	17

T

technical assistance	11
trademarks and service marks.	10
Training	16

U

Unified Communication Center	53
Host ID	54
License file information	55
Upgrades	36
User requirements	13

V

Value Types	17
Virtual Private Networking.	33
Voice Self Service	55
License file information	56